Commonwealth Information Security Council – Encryption Sub-Committee

Meeting 9/24/07
Attendees: Michael McDaniel, Tripp Simms, Steve Werby
Committee members: Jesse Crim (VCU), John Palese (DSS), Michael McDaniel (VRS), Tripp Simms (VITA/NG), Steve Werby (DOC), Craig Goeller (DMAS)

I'll try to summarize today's meeting; anyone present, please add or correct to my points below.

In the Council meeting, there were two other groups that also wanted to do surveys. It was decided that there will be one survey for the entire Council. The survey will go out to the ISO's and copied to the AITR's as FYI. The thought was to have about 6 questions from each sub-committee.

VRS has an on-line survey system (NSurvey) and we can use this for our survey. I've setup a sample survey at:
http://survey.vrs.virginia.gov/nsurvey.aspx?surveyid=693ae4491114c05a4b33da6b810ccea&uid=01619c25-950d-4906-be80-020ddd2d42ff

As an intro to our survey questions we need a small paragraph on how they will benefit from the survey. Like:

> By collecting this data it will help determine agencies encryption needs and current deployment status. With this knowledge we can develop a tool to assist agencies with the encryption technology and provide guidance on available solutions.

It was suggested not to use the word "encryption" in the survey.

Part of the educating users goal, could be a guide to citizens on encryption.

How do we get the ISO's to respond to the survey? Possibly list the responding agencies in the ISOAG meetings.

Independently we all need to come up with a few questions. Look at encryption technology solutions as you think of the questions.

**** Goal *** Due by October 19 (Friday) *** Questions for the Survey. Once we have the combined questions we can then refine them and narrow them down. By meeting this date we can have the final ready by then end of October (meeting the council's goal).**

Questions (from this meeting and previous meeting):

> Does your agency send sensitive information to people outside your agency (external customers)?

Data at rest…
Do workers store sensitive information on laptop or notebook computers?
Do workers store sensitive information on portable storage devices such as diskettes, floppy disks, CDs, flash drives, etc.
Do workers send sensitive information over the Internet?
Does your agency have a need for secure file transfer (e.g. SSH, SFTP, etc)?
Do workers need secure remote access (e.g. VPN)?
Is secure login or administration required (e.g. SSH, SSL)?
Are digital signatures required?
Is wireless security required?
Is VOIP security required?
For each question, please list the products that are currently in use.
How sensitive information is used, stored and sent.
What is the level of technical expertise of the individuals who will be using encryption?
What encryption solutions are you implementing today and what would you like to be able to do tomorrow?
Do you know that you are not to send Sensitive data through email?
Tripp, you had some additional questions that I did not capture, can you add those here.

*** Cumulative Notes from all meetings ***

Recap from previous meetings:
The goals:

- **Survey agencies – IT and business perspective**
- **Develop plan for educating users and ISOs**
- **Develop best practices and compare with Commonwealth's practices**
- **Recommend feature sets for enterprise encryption solutions**

Survey agencies

- Create a series of questions to help agencies determine whether they have a particular encryption need and provide guidance on solutions.
- Re-survey agencies with questions designed to describe: 1)how sensitive information is used, stored and sent and 2)the level of technical expertise of the individuals who will be using encryption
- Qualitative and quantitative survey of ISO and an executive level manager from agencies on current state, risks, needs, etc. to prioritize strategy and to develop benchmarks for future comparison and measurements
-
- Discussed who will be the possible targets (i.e. ISO's, agency heads)
- Discussed methods of delivery (email, online survey, handouts during ISOAG meeting)
- Include a data dictionary to define terms on the survey and help guide them through the survey

- Task: Steve is going to send around the previous VITA survey so that we can begin to analyze those questions; making changes, additions, or removal. Will use information gathered from best practices to help develop the Questionnaire.
- With the answers from the Questionnaire, Best Practices, and Recommend Solutions we could come up with a chart to aid agencies in determining encryption needs and solutions.

Develop plan for educating users and ISOs

- How to educate your employees on encryption
- To include appropriate training material
-
- Develop written education material agencies can use as template for security awareness programs
- Educate technical/decision makers on the types of available encryption, and negatives/positives of each
- Plan for educating / selling executive level management on all types of encryption based on risk and business value

Develop best practices and compare with Commonwealth's practices

- Conduct research and meet with other professionals inside and outside government in order to develop best practices
- Provide written guidance on policies and best practices (lower level than VITA guidelines/policies/standards) for ISOs of state agencies
- Deployment scenarios
- What to avoid
-
- We thought about a new goal to look at the Commonwealth Policy and Standards on encryption, but decided to add it as part of the outcome of developing best practices.
- Task: Tripp is going to pull together some standards and guidelines from NIST, Gartner, and IDefense and send those to the group.
- Other sources to check out other sites such as other State Government sites, Va Affairs, California, etc.
- Research and/or provide links to sources of reviews on the strengths of various encryption packages.
- <u>*Developing these best practices will be the primary focus of our next meeting.*</u>

Recommend feature sets for enterprise encryption solutions

- Changed the title of the goal. We can not recommend a product.
- Could offer a resource in the form of listing feature sets and capabilities. (i.e. If you want to do this type of encryption…then look for a product with this feature set…)

- We had discussion on NG and the partnership and their role in encryption. That the partnership may or may not choose to follow our guidelines, and not to let what NG is deploying or planning influence our outcomes.

We need to define Sensitive Information for our survey:
Sensitive Information is defined as personal identifiable information such as names, address, social security number and telephone number.

Research links provided by Tripp:

Data Classification:
These look useful to me for use in the questionnaire in helping ISOs, and the agencies they represent, determine the appropriate classification levels for their data. I've included them particularly because their presentation was easy to follow.

Secure Computing: Stanford Data Classification Guidelines
http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html
Summary: Criteria for determining appropriate data classification

Categorizing Data Sensitivity for Computer Security
http://datacenter.cit.nih.gov/interface/interface222/security.html
Summary: Specific to NIH, but its nicely formatted and simple to follow.

IT Security Cookbook - 4 Information Classification
http://www.boran.com/security/IT1x-4.html#Heading37
Summary: Much the same formula as NIH, but geared toward a general audience.

Data Encryption Policies and Guidelines:
Should be useful in putting together a framework for our document(s).

UT at Austin:Data Encryption Guidelines
http://www.utexas.edu/its/policies/opsmanual/encrypt-guide.php
Summary: Reads like a cross between a policy and a guideline, still worthwhile.

Encryption at the University of California: Overview and Recommendations
http://www.ucop.edu/irc/itsec/uc/EncryptionGuidelinesFinal.html
Summary: Very well put together document, could see using it as a framework for our own.

Ohio:ITB-2007.02 Data Encryption and Securing Sensitive Information
http://oit.ohio.gov/IGD/policy/pdfs_bulletins/ITB-2007.02.pdf
Summary: Heh, I had to include Ohio! :)

Misc:
Supporting documents...

NIST:FIPS 140-3:Security Requirements for Cryptographic Modules
Overview: http://csrc.nist.gov/cryptval/140-3.htm
Document: http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf
Summary: Technical document regarding security levels for cryptographic subsystems

NIST:FIPS 199:
Standards for Security Categorization of Federal Information and Information Systems
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Summary: NIST FIPS for Federal requirements regarding data classification

PGP:Sarbanes-Oxley Act:Data Security and Encryption
http://download.pgp.com/pdfs/whitepapers/Regulation_SOX_040416_FL.pdf
Summary: PGP Corporations recommendations on SOX guidelines and requirements

This is the summary of the previous encryption survey:


Agency_Survey_Summary.doc

Although we are remaining vendor neutral, I have attached a short list of vendors that has encryption products:
Liquid Machines
Credant
PointSec
PGP
Microsoft EFS/BitLocker
Guardian Edge
Utimaco
SecureStar DriveCrypt disk encryption
TrueCrypt

Gartner Magic Quadrant for Mobile Data Protection 2007

magic_quadrant_for_mobile_da_151075.p